AMENDMENTS TO THE CLAIMS

The following listing of claims replaces all prior versions of the claims and all prior listings of the claims in the present application.

1. (canceled)

2. (currently amended) A multiple modulus selector of a computer system, communication network, or computer system and communication network that uses a public-key cryptographic algorithm, the multiple modulus selector comprising:

a modulus recoder adapted to receive an n-bit modulus M, a previous sum, and a current partial product to generate a first selection signal;

a modulus selector adapted to receive the n-bit modulus M, the previous sum, the current partial product, and a multiplicand to generate a second selection signal; and

a multiplexer adapted to receive inputs -M, 0, M, and 2M, adapted to select one of the inputs -M, 0, M, and 2M based on the first selection signal in an integer modular multiplication mode, and adapted to select one of the inputs -M, 0, M, and 2M based on the second selection signal in a polynomial modular multiplication mode;

wherein the multiple modulus selector is used in the public-key cryptographic algorithm.

3. (previously presented) The multiple modulus selector of claim 2, wherein the input -M is obtained by inverting the modulus M.

4. (previously presented) The multiple modulus selector of claim 2, wherein the input 2M is obtained by shifting the modulus M.

5. (previously presented) The multiple modulus selector of claim 2, wherein the modulus M is stored in a register.

6. (previously presented) The multiple modulus selector of claim 2, wherein the modulus recoder further generates a multiple modulus negation indicating signal that is input to an accumulator.

7. (previously presented) The multiple modulus selector of claim 2, wherein the n-bit modulus M includes a second least significant bit and a sum of the previous sum and current partial product.

8. (previously presented) The multiple modulus selector of claim 2, wherein the first selection signal includes two bits.

9. (previously presented) The multiple modulus selector of claim 2, wherein the modulus selector further generates a multiple modulus accumulation indicating signal that is input to an accumulator.

10. (previously presented) The multiple modulus selector of claim 2, wherein the multiplicand includes two bits.

11. (previously presented) The multiple modulus selector of claim 2, wherein the second selection signal includes two bits.

12. (currently amended) A Montgomery modular multiplier of a computer system, communication network, or computer system and communication network that uses a public-key cryptographic algorithm, the Montgomery modular multiplier comprising:

a multiple modulus selector adapted to select one of -M, 0, M, and 2M (M being an n-bit modulus number) as a multiple modulus in an integer modular multiplication mode, and adapted to select one of 0, M, and 2M as a multiple modulus in a polynomial modular multiplication mode to output a multiple modulus accumulation indicating signal;

a Booth recoder adapted to provide a first value used to obtain a partial product value; and

an accumulator adapted to sum second values to obtain a result of the Montgomery multiplier;

wherein the accumulator sums the modulus M and the second values based on the multiple modulus accumulation indicating signal in the polynomial modular multiplication mode;

wherein the Montgomery modular multiplier is used in the public-key cryptographic algorithm.

13. (previously presented) The Montgomery multiplier of claim 12, further comprising:

a modulus number register adapted to store a modulus value in the modulus number register;

a multiplicand register adapted to store a multiplicand value in the multiplicand register;

a multiplicator register adapted to store a multiplicator value in the multiplicator register;

an AND gate adapted to combine the multiplicator value with the multiplicand value; and

two adders adapted to combine the values from the accumulator and the AND gate to output a combined value;

wherein the combined value is input to the multiple modulus selector.

14. (previously presented) The Montgomery multiplier of claim 12, wherein the multiple modulus selector comprises:

a modulus recoder adapted to receive an n-bit modulus M, a previous sum, and a current partial product to generate a first selection signal;

a modulus selector adapted to receive the n-bit modulus M, the previous sum, the current partial product, and a multiplicand to generate a second selection signal; and

a multiplexer adapted to receive inputs -M, 0, M, and 2M, adapted to select one of the inputs -M, 0, M, and 2M based on the first selection signal in an integer modular multiplication mode, and adapted to select one of the inputs 0, M, and 2M based on the second selection signal in a polynomial modular multiplication mode.

15. (previously presented) The Montgomery multiplier of claim 12, wherein the Booth recoder comprises:

a first selector adapted to receive a multiplicator to generate a third selection signal;

a second selector adapted to receive the multiplicator to generate a fourth selection signal; and

a multiplexer adapted to receive inputs -2A, -A, 0, A, 2A, adapted to select one of the inputs -2A, -A, 0, A, 2A based on the third selection signal in an integer modular multiplication mode, and adapted to select one of the

inputs 0, A, and 2A based on the fourth selection signal in a polynomial modular multiplication mode.

16. (canceled)

17. (currently amended) A Booth recoder of a computer system, communication network, or computer system and communication network that uses a public-key cryptographic algorithm, the Booth recoder comprising:

a first selector adapted to receive a multiplicator to generate a first selection signal;

a second selector adapted to receive the multiplicator to generate a second selection signal; and

a multiplexer adapted to receive first inputs -2A, -A, 0, A, 2A, adapted to select one of the first inputs -2A, -A, 0, A, 2A based on the first selection signal in an integer modular multiplication mode, adapted to receive second inputs 0, A, and 2A, and adapted to select one of the second inputs 0, A, and 2A based on the second selection signal in a polynomial modular multiplication mode;

wherein the Booth recoder is used in the public-key cryptographic algorithm.